

ABSTRACT

A method and system for structuring an object in security policies of a computer system includes: receiving a request to access a virtual volume with a virtual name; mapping the virtual name to the real object; and providing the real object. The method and system uses virtual objects which map to real objects in a computer system. The access control mediator grants or denies access to a virtual object using a discretionary or a mandatory policy. A virtual name is mapped to a real object. This mapping is transparent to the subject. In this manner, security policies can be enforced over objects stored in file systems without regard to the policies of the file systems. The system can also be used as a gateway to remote file systems built on top of existing file systems. These advantages provide more flexibility in controlling a subject's access to real objects.